**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MASSACHUSETTS**

| | |
|---|---|
| ERICA BAKER, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>PROGRESS SOFTWARE CORPORATION,<br><br>Defendant. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Erica Baker ("Plaintiff") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to herself and on information and belief as to all other matters, brings this Class Action Complaint against Defendant Progress Software Corporation ("PSC"), and in support thereof alleges as follows:

## NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of herself and all other individuals ("class members"), totaling more than 37 million people and 550 organizations, who had their sensitive personal identifiable information ("PII") and protected health information ("PHI")—as defined by the Health Insurance Portability and Accountability Act ("HIPPA")—accessed and hacked by malicious, unauthorized third parties that accessed and removed the PII and PHI from Defendant's systems as early as May 27, 2023[1] (the "Data Breach").

2. PSC advertises itself as an "experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."[2]

[1] https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-researchers-say-2023-06-02/ (last visited July 19, 2023).
[2] https://www.progress.com/company (last visited July 19, 2023).

3. PSC offers both solutions and products, including its file transfer service called MOVEit, which "provides secure collaboration and automated file transfers of sensitive data and advanced workflow automation capabilities without the need for scripting. Encryption and activity tracking enable compliance with regulations such as PCI, HIPAA and GDPR."[3]

4. Specifically, PSC describes MOVEit as a "managed file transfer software" that PSC claims is a "leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over file transfer activities. Whether deployed as-a-Service, in the Cloud, or on premises, MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[4]

5. MOVEit is used by more than 1,700 software companies and 3.5 million users worldwide.[5]

6. PSC's wholly-owned subsidiary, Ipswitch, Inc. ("Ipswitch"), developed MOVEit along with other products that "enable small and medium sized business and enterprises to provide secure data sharing and ensure high-performance infrastructure" and was acquired by PSC in 2019.[6]

7. PSC's website states[7]:

> to comply with HIPAA, Progress operates secure computing environments in its corporate offices, development environments, and production cloud products. Each

[3] https://www.progress.com/moveit (last visited July 19, 2023).
[4] https://www.ipswitch.com/moveit?_ga=2.178322852.1251772019.1689781398-357640369.1688748444 (last visited July 19, 2023).
[5] https://www.jdsupra.com/legalnews/moveit-transfer-zero-day-vulnerability-9280864/#:~:text=With%20more%20than%201%2C700%20software,unidentified%20threat%20actor%20groups%20worldwide (last visited July 19, 2023).
[6] https://investors.progress.com/news-releases/news-release-details/progress-acquire-ipswitch-inc (last visited July 19, 2023).
[7] https://www.progress.com/legal/hipaa-compliance-faqs (last visited July 19, 2023).

> of these areas are equipped with security technologies, processes, and people needed to protect sensitive information. The Progress Internal Audit team audits use of security solutions and processes, evaluated by annual SOC2 assessments and validated by annual HIPAA audits. Copies of the SOC2 assessments and audit reports are available to our customers upon request. Progress corporate administration and human resources functions are also audited for HIPAA compliance on an annual basis.

8. PSC's website states that "within our Sites, you may be asked to give us personal or organizational information in order to purchase or receive information about a Progress Property. We may collect this information through different methods."[8]

9. PSC's website further states that "in some cases, end users of our customers may need to provide Sensitive Personal Information to our customer in order to make use of an application that uses our Product or SaaS Product and that Sensitive Personal Information may be stored or processed by us as a result. We process such Sensitive Personal Information in the role of a processor on behalf of a customer (and/or its affiliates) who is the responsible controller of the Sensitive Personal Information concerned."[9]

10. PSC notes that "the Personal Information collected by Progress Software may include, but is not necessarily limited to:

- Contact information (such as your name, title, e-mail address, postal address, and telephone number);
- Transactional information, including delivery details, including billing and delivery address where applicable;
- User preferences;
- IP address;
- Financial/credit card and payment information (please see the "Third Party Payment Processor" section for more information);
- Demographic information and geographic or geo-location information; and

[8] https://www.progress.com/legal/privacy-policy (last visited July 19, 2023).
[9] *Id*.

- Additional information as needed for our business and customer service purpose"[10]

11. On or around May 31, 2023, PSC discovered and reported a vulnerability in its MOVEit Transfer and MOVEit Cloud systems that "could lead to escalated privileges and potential unauthorized access." On or about that same day, PSC purportedly notified all customers, and developed and released a security patch with 48 hours.[11] PSC assigned a severity rating of 9.8 out of 10 to this vulnerability.[12]

12. On or around June 9, 2023, PSC and its contracted cybersecurity firm, Huntress, uncovered additional vulnerabilities "distinct from the previously reported vulnerability shared on May 31, 2023."[13]

13. It has been reported that the Data Breach affecting PSC's MOVEit software is unique from most other recent data breaches because MOVEit is widely used, and the Breach impacted both primary users of the software, as well as their contracted third parties that also use the software.[14]

14. It has been reported that the Data Breach was a ransomware attack conducted by a notorious ransomware group, C10p, which claims to have committed the Data Breach.[15]

---

[10] *Id*.
[11] https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability (last visited July 19, 2023).
[12] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (last visited July 19, 2023).
[13] *Id*.
[14] *Id*.
[15] *Id*.

15. C10p claims to have stolen PII and PHI information from over 550 organizations and 37 million individuals, including U.S. schools, the U.S. public sector, and the U.S. private sector.[16]

16. C10p is a well-known ransomware group, which "[has] been linked to FIN11, a financially-motivated cybercrime operation" and is "connected to both Russia and Ukraine and which is believed to be part of a larger umbrella operation known as TA505."[17]

17. It has been reported that C10p has requested unspecified ransom from the impacted organizations in exchange for C10p to abstain from releasing consumers' highly sensitive PII and PHI. As of July 19, 2023, C10p and its hacking of MOVEit has resulted in the theft of more than 37 million individuals' sensitive information.[18] Because the Data Breach was conducted by known, self-proclaimed ransomware hackers, Plaintiff's and class members' sensitive PII and PHI are irrefutably in the possession of known bad actors.

18. PSC owed a duty to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII and PHI against unauthorized access and disclosure. PSC breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII and PHI entrusted to it from unauthorized access and disclosure.

19. As a result of PSC's inadequate security and breach of its duties and obligations, the Data Breach occurred and Plaintiff's and class members' PII and PHI was accessed by, and disclosed to, an unauthorized third-party actor. This instant action seeks to remedy these failings and their consequences. Plaintiff thus brings this complaint on behalf of herself and all similarly

[16] *Id.*
[17] *Id.*
[18] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html

situated individuals whose PII and/or PHI was exposed as a result of the Data Breach, which PSC learned of on or about May 27, 2023, but did not publicly disclose until May 31, 2023.

20. Plaintiff, on behalf of herself and all other class members, asserts claims for negligence, negligence per se, invasion of privacy, unjust enrichment, and violations of the Illinois Personal Information Protection Act ( 815 ILCS 530/10(a)), and seeks declaratory and injunctive relief, monetary damages including punitive damages, equitable relief, and all other relief authorized by law.

## PARTIES

### A. Plaintiff Erica Baker

21. Plaintiff Erica Baker is a resident and citizen of the state of Illinois and resides in Dolton, Illinois.

22. Plaintiff received a letter from the Illinois Department of Innovation and Technology dated June 28, 2023, confirming that her PII and PHI were impacted by the Data Breach and accessed by cybercriminals that accessed Defendant's systems:

> The breach involved foreign cybercriminals and impacted thousands of businesses, organizations and government agencies worldwide. It occurred through a vulnerability in a software product provided by MOVEit, a third-party file transfer company. The cybercriminals exploited the vulnerability and stole files that contained your personally identifiable information, PI (information that may include your name, address, and Social Security Number), protected health information, PHI information that may be clinical, demographic and financial in nature). The cyberattack affected the State of illinois Cepartment of Innovation and Technology (DolT), which is the information technology agency for many state agencies.

23. Prior to retaining counsel for claims related to the Data Breach, Plaintiff spent at least an hour monitoring her accounts for fraudulent activity and identity theft. She will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

**B. Defendant Progress Software Corporation**

24. Defendant Progress Software Corporation is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803.

## JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more class members are citizens of states different from Defendant.

26. The Court has personal jurisdiction over Defendant because it maintains its principal place of business in this judicial District, conducts significant business in Massachusetts, and/or otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Massachusetts.

27. Venue properly lies in this District because, *inter alia,* Defendant maintains its principal place of business in this judicial District; transacts substantial business, has agents, and is otherwise located in this District; and/or a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial District.

## FACTUAL ALLEGATIONS

**A. Overview of Defendant**

28. PSC advertises itself as "the experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."[19]

[19] https://www.progress.com/company (last visited July 19, 2023).

29. PSC offers both solutions and products, including MOVEit, which "provides secure collaboration and automated file transfers of sensitive data and advanced workflow automation capabilities without the need for scripting. Encryption and activity tracking enable compliance with regulations such as PCI, HIPAA and GDPR."[20]

30. MOVEit is a "managed file transfer software" that PSC claims is "leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over file transfer activities. Whether deployed as-a-Service, in the Cloud, or on premises, MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[21]

31. PSC claims MOVEit has "flexible architecture makes it easy to choose the exact capabilities that match your organization's specific needs,"[22] which include three modules:

- **MOVEit Cloud** – "MOVEit Cloud enables the consolidation of all file transfer activities to one system to ensure better management control over core business processes. A trusted and proven SaaS solution, it provides full security, reliability and compliance with the convenience of a cloud-based service. It provides the security, centralized access controls, file encryption and activity tracking needed to ensure operational reliability and compliance with SLAs, internal governance and regulatory requirements like PCI, HIPAA, CCPA/CPRA and GDPR."[23]
- **MOVEit Transfer** – "MOVEit Transfer provides the same award-winning capabilities

[20] https://www.progress.com/moveit (last visited July 19, 2023).
[21] https://www.ipswitch.com/moveit?_ga=2.178322852.1251772019.1689781398-357640369.1688748444 (last visited July 19, 2023).
[22] *Id.*
[23] *Id.*

of MOVEit Cloud in an on-premises solution. Ensure management and control over your business-critical file transfers by consolidating them all on one system. Leverage MOVEit Transfer's file encryption, security, activity tracking tamper-evident logging, and centralized access controls to meet your operational requirements. Reliably and easily comply with SLAs, internal governance requirements and regulations like PCI, HIPAA, CCPA/CPRA and GDPR."[24]

- **MOVEit Automation** – "MOVEit Automation works with MOVEit Cloud, MOVEit Transfer to let admins and authorized users easily create file-based tasks without programming. It automates and controls access to file transfer resources, minimizes workloads and reduces errors while mitigating the risk of data loss. You get a reliable, secure means of sharing business data with an audit trail and visibility into all file transfer activities."[25]

32. MOVEit is used by more than 1,700 software companies and 3.5 million users worldwide.[26]

33. Ipswitch developed MOVEit along with other products that "enable small and medium sized business and enterprises to provide secure data sharing and ensure high-performance infrastructure" and was acquired by PSC in 2019.[27]

34. Discovery will show that through its provision of the foregoing services, PSC obtains possession of its customers'—including Plaintiff's and class members'—highly sensitive

[24] *Id*.
[25] *Id*.
[26] https://www.jdsupra.com/legalnews/moveit-transfer-zero-day-vulnerability-9280864/#:~:text=With%20more%20than%201%2C700%20software,unidentified%20threat%20actor%20groups%20worldwide (last visited July 19, 2023).
[27] https://investors.progress.com/news-releases/news-release-details/progress-acquire-ipswitch-inc (last visited July 19, 2023).

PII and PHI. Thus, in the regular course of its business, PSC collects and maintains the PII and PHI of consumers. Upon information and belief, that information ordinarily includes: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) driver's license numbers or other state-issued ID numbers, (4) insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (5) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); (6) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by the provider); and (7) information of any parent, guardian, or guarantor. Defendant stores this information digitally in the regular course of business.

35. PSC's website assures viewers that its MOVEit service is safe and secure: "[MOVEit] is the experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, **then manage it all safely and securely**."[28]

36. PSC's website states that its MOVEit product allows for the secure transfer of sensitive information, in particular, in compliance with HIPAA and industry privacy standards: "[MOVEit] provides **secure** collaboration and automated file transfers of **sensitive data** and advanced workflow automation capabilities without the need for scripting. Encryption and activity tracking **enable compliance with regulations such as PCI, HIPAA and GDPR**."[29]

[28] https://www.progress.com/company (last visited July 19, 2023).
[29] https://www.progress.com/moveit (last visited August 3, 2023).

37. Likewise, PSC advertises its MOVEit product as a way to "**securely share files** across the enterprise and globally" and "transfer[s] **sensitive information securely**" while "let[ting] end users collaborate securely."[30]

**Everyone's demanding security and compliance, but nobody's giving you the resources to make it happen.**

The federal government passes sweeping legislation like HIPAA and HITECH. State governments follow suit with mandates such as the Standards for The Protection of Personal Information of Residents of the Commonwealth (applicable in Massachusetts). The regulators oversee your organization as they enforce the laws. And your organization's leadership team promises to comply. But then...an over-eager end user who insists on an "easy, fast" workaround makes a totally avoidable PICNIC (Problem in Chair Not In Computer) mistake that leads to file security being compromised.

You're the one who's asked to fix the problem. And what a problem it is: If you can't produce the right files at the right time, or if you can't prove they were properly protected, your organization could be subject to millions of dollars in government fines and penalties, a battered reputation in the healthcare community, and a loss of trust by medical professionals, patients, and the public at large.

38. PSC advertises its MOVEit product as a secure Managed File Transfer (MFT) system that allows users to transfer data securely, in complete fulfillment of their compliance requirements[31]:

> [MOVEit] allows you to meet your growing (and increasingly complex) file transfer needs. It can be delivered to your doorstep neatly and simply. And **it enables you to transfer files reliably and securely**, meet all your all-important compliance requirements, eliminate manual workflows, and provide end users with an IT-approved solution for sending files. MFT also guarantees you visibility and control over all file transfer activities, enables you to confidently meet your SLAs, and provides you with easy implementation/on-boarding.

---

[30] *Id.*

[31] https://www.ipswitch.com/resources/best-practices/secure-healthcare-file-transfer (last visited August 3, 2023).

39. Defendant's website states further:

> Specifically, with MOVEit from Progress you'll receive four vital benefits that are unavailable with the all-too-common array of legacy systems:
>
> - Connectivity ensures that end users can access the system via mobile devices, email, or a web browser. IT retains control yet workers maintain high levels of productivity through easy-to-use, flexible access.
> - Administration so that you can easily set up, control, and manage your organizational file transfers, provision users/accounts easily, and onboard partners and control access.
> - Automation to make sure that files route appropriately according to key business processes and they integrate into other applications for scheduling and routing.
> - Reporting for enterprise visibility and control, compliance and governance and to easily provide reports for auditing and regulatory inquiries.

40. In its whitepaper "7 Steps to Compliance with Data Protection Laws", PSC acknowledges that organizations that transfer and store PI and PHI face serious threats to ensuring the integrity of that information[32]:

> Stolen Personal Information (PI) drives a thriving black market for cybercriminals on a global basis. Since PI includes any data which can be used to identify an individual, every organization that collects data such as passwords, credit card data, health information and addresses is a potential target for cybercriminals. Not surprisingly, since 2013 data breaches have accounted for nearly 6 billion stolen data records globally. Also not surprisingly, governments around the world have responded with increasingly strict regulations regarding the collection, retention, processing and sharing of PI. Failure to comply with these regulations can result in severe fines.

41. PSC is well aware of its legal obligations and industry standard-imposing duties to protect consumers' sensitive PII and PHI because in this white paper, PSC details seven best practices for ensuring data integrity and meeting compliance with data protection laws:

[32] This whitepaper can be accessed through the following link: https://www.ipswitch.com/resources/whitepapers-ebooks/7-steps-to-data-protection-law-compliance (last visited August 3, 2023).

1

AUTOMATION

Commonly used file transfer workflows should be automated to mitigate against the introduction of human error that might result in data loss. Your file transfer tools should support functions such as automatic forwarding, error correction, and confirmation of receipt for all data transfers.

2

CONTROL AND VISIBILITY

Control and visibility of transfer activities are important security requirements and essential for validating compliance. Your tools should enable central visibility, control and prior authorization of all file transfers. Logs should be kept in a tamper-evident database to assure the integrity of audit trails.

3

INFORMATION SECURITY

Your technology, tools or processes should ensure file integrity checks, data deletion after receipt, and non-repudiation (the sender and receiver are both authorized and authenticated to access the data). They should provide an automated audit trail that tracks integrity, delivery and authentication

4

AUTHENTICATION

Effective authentication of users and administrators is an essential control. Your file transfer systems should accommodate an array of access control mechanisms, including integration with central user directories, role-based access control and single sign-on as well as multi-factor authentication.

5

CRYPTOGRAPHY

Encryption algorithms have a limited shelf life. Compliance standards often do not allow the use of compromised systems. It is essential that your systems employ strong, state-of-the-art cryptographic mechanisms and enable secure selection, distribution and protection of encryption keys.

6

SECURE ARCHITECTURE

Your systems architecture should integrate with existing security infrastructures and applications. The systems should also either ensure that there is no unencrypted data within the DMZ or provide for DMZ termination of inbound requests for authentication and data transfer with a gateway proxy server.

7

FAILOVER

A key requirement of many data protection regulations is secure business continuity. This requirement is meant to safeguard the confidentiality, integrity and availability of file transfers, at all stages throughout any failures, disasters or outages. Automatic, secure failover is essential to ensure that file transfers are either successful or continuously restarted until complete.

42. In this white paper, PSC emphasizes the security of MOVEit, and advertises it as a MFT system that can address "each of the seven core best-practices for compliance with data

protection regulations"[33]:

## MOVEit Compliance Features

MOVEit® is a Managed File Transfer system that lets you manage, view, secure, and control the exchange of sensitive data with external parties to assure compliance with data protection regulations. The table below shows how MOVEit addresses each of the seven core best-practices for compliance with data protection regulations.

| Security Requirement | MOVEit Control |
|---|---|
| Compliance | MOVEit helps ensure that file transfers are secured, data is protected at all times, and records of transfers are secured in tamper-proof audit trails for legally required periods prior to assured destruction. |
| Communications Security | MOVEit enables central visibility, control and prior authorization of all file transfers, as well as encryption, traceability and non-repudiation of transfers, including secure audit trails of significant events. MOVEit is architected to integrate with existing security infrastructure, policies, and applications, ensuring there is no unencrypted data in the DMZ and eliminating any requirement for external access. |
| Information Security Policies | MOVEit encrypts files at rest and in transit, provides non-repudiation and file integrity checks. Ipswitch provides email, web, mobile access and desktop clients which, when used with MOVEit provide compliant file transfer access to all users. |
| Access Control | MOVEit offers a choice of authentication mechanisms, including integrations with existing systems, and a rich set of features to support user access management, including blacklists and whitelists, and tools to help administrators select the most appropriate settings to meet security policies. |
| Cryptography | MOVEit employs strong cryptographic mechanisms and secure selection, distribution and protection of encryption and decryption keys, consistent with international legal and regulatory requirements. |
| Physical & Environmental Security | MOVEit provides flexibility in implementation to ensure adherence to local physical security requirements. |
| Business Continuity Security | MOVEit safeguards the confidentiality, integrity and availability of file transfers at all stages throughout any failures, disasters or outages. Ipswitch Failover can assure uninterrupted file transfer processing. |

43. PSC's Privacy Policy posted on its website notes that PSC is committed to protecting the privacy of individuals[34]:

[33] *Id.*

[34] https://www.progress.com/legal/privacy-policy (last visited August 3, 2023).

> Progress Software Corporation, together with its subsidiaries and affiliates, ("Progress", "we", "us", "our" or the "Company") is committed to protecting the privacy of individuals who visit the Company's web sites, individuals who register to use our services, and individuals who register to attend the Company's corporate events. This Privacy Policy (the "Policy") describes Progress' privacy practices in relation to the use of the Company's web sites and the related applications, services, and programs offered by the Company, as well as individuals' choices regarding use, access and correction of personal information.

44. PSC's Privacy Policy promises consumers that it has systems and processes in place to ensure the security and privacy of their sensitive PII and PHI, in compliance with governing law and industry standards[35]:

> **Our Security Practices**
>
> Progress employs industry standard security measures to ensure the security of information. However, the security of information transmitted through the Internet can never be guaranteed. Progress is not responsible for any interception or interruption of any communications through the internet or for changes to or losses of information. Users of our Sites are responsible for maintaining the security of any password, user ID, or other form of authentication involved in obtaining access to password protected or secure areas of any of our websites. To protect you and your information, Progress may suspend your use of a website, without notice, pending an investigation, if any breach of security is suspected. Access to and use of password protected and/or secure area of any Progress Software site is restricted to authorized users only. Unauthorized access to such areas is prohibited and may lead to criminal prosecution.
>
> We have put in place physical, electronic, and managerial procedures designed to help prevent unauthorized access, to maintain data security, and to use correctly the Information we collect online. These safeguards vary based on the sensitivity of the information that we collect and store. We also use administrative, technical, and physical security measures to help protect your personal information. While we have taken reasonable steps to secure the personal information you provide to us, please be aware that despite our efforts, no security measures are perfect or impenetrable, and no method of data transmission can be guaranteed against any interception or other type of misuse. Any information disclosed online is vulnerable to interception and misuse by unauthorized parties. Therefore, we cannot guarantee complete security if you provide personal information.

[35] https://www.progress.com/legal/privacy-policy (last visited August 3, 2023).

45. PSC's Privacy Policy assures consumers that it will not share their sensitive information—which necessarily includes by letting a data breach access it—without first obtaining the consumers' written consent:

> Notwithstanding the above, if we ever need to handle Sensitive Personal Information about you, we will ask your consent to do so. Once given, such consent may be withdrawn at any time. We will not handle any Sensitive Personal Information that we are not permitted by you to handle, or that you have not provided us with. Any Personal Information about you that we handle will only be accessible by those Progress personnel who have a reason to do so.[36]

> With your consent (when required), we may use and share the Personal Information we collect to: provide, support and improve the Progress Properties; deliver correspondence, communications, or services, such as newsletters, events, training, or software that you request or purchase; process orders; confirm licensing compliance; solicit your feedback; and inform you about the Company and the products and services of our distributors, resellers and promotional partners.[37]

46. PSC acknowledges that some of its products are Covered Entities under HIPAA and thus are required to entire into Business Associate Agreements.[38]

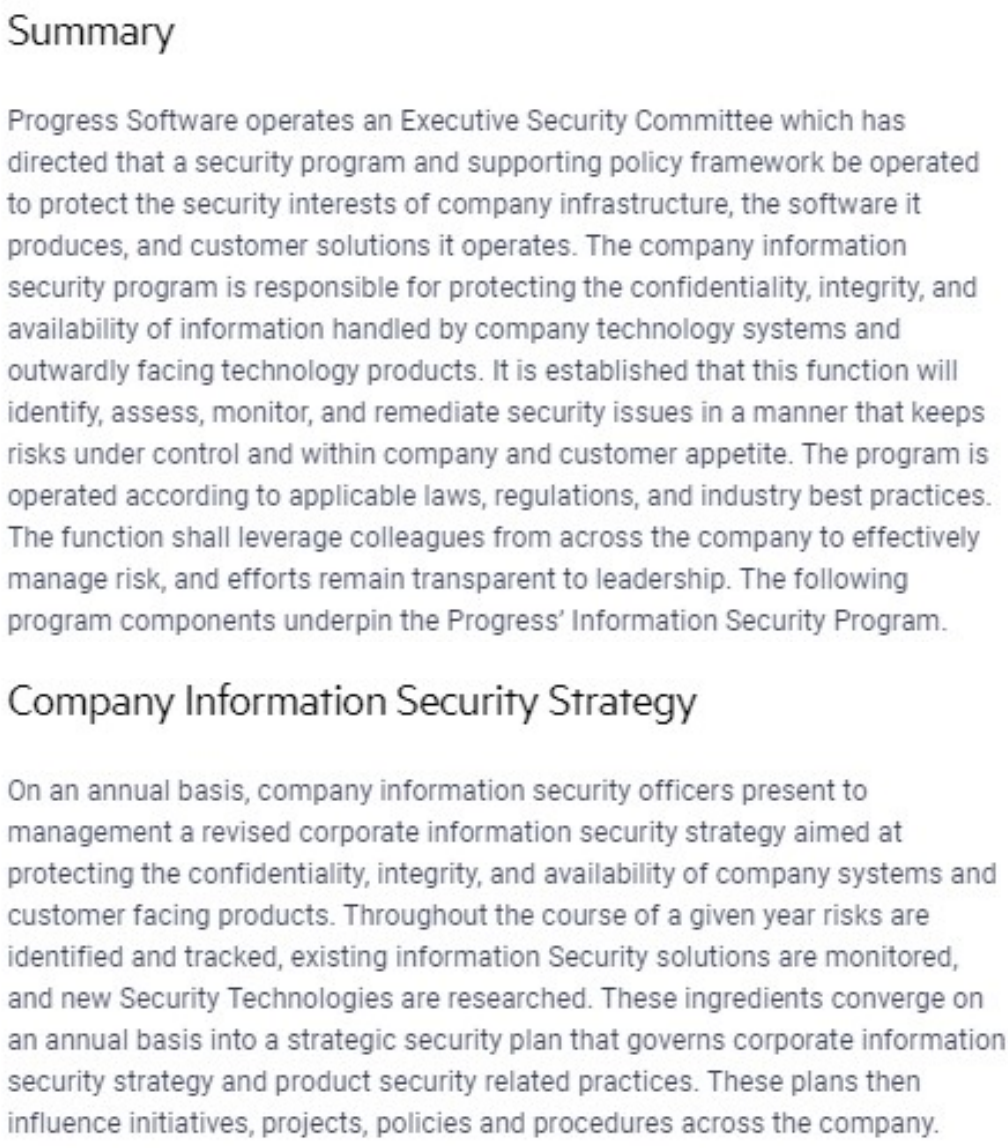
47. PSC acknowledges that it has a legal duty to safeguard PII and PHI under HIPAA and takes the following steps to meet its legal obligations[39]:

> To comply with HIPAA, Progress operates secure computing environments in its corporate offices, development environments, and production cloud products. Each of these areas are equipped with security technologies, processes, and people needed to protect sensitive information. The Progress Internal Audit team audits use of security solutions and processes, evaluated by annual SOC2 assessments and validated by annual HIPAA audits. Copies of the SOC2 assessments and audit reports are available to our customers upon request. Progress corporate administration and human resources functions are also audited for HIPAA compliance on an annual basis.

---

[36] *Id.*
[37] *Id.*
[38] https://www.progress.com/legal/hipaa-compliance-faqs (last visited August 3, 2023).
[39] *Id.*

48. PSC further assures consumers that as an additional measure to ensure data integrity, it implements and maintains an Executive Security Committee, which conducts annual audits of its systems, among other things, to identify vulnerabilities:[40]



Summary

Progress Software operates an Executive Security Committee which has directed that a security program and supporting policy framework be operated to protect the security interests of company infrastructure, the software it produces, and customer solutions it operates. The company information security program is responsible for protecting the confidentiality, integrity, and availability of information handled by company technology systems and outwardly facing technology products. It is established that this function will identify, assess, monitor, and remediate security issues in a manner that keeps risks under control and within company and customer appetite. The program is operated according to applicable laws, regulations, and industry best practices. The function shall leverage colleagues from across the company to effectively manage risk, and efforts remain transparent to leadership. The following program components underpin the Progress' Information Security Program.

Company Information Security Strategy

On an annual basis, company information security officers present to management a revised corporate information security strategy aimed at protecting the confidentiality, integrity, and availability of company systems and customer facing products. Throughout the course of a given year risks are identified and tracked, existing information Security solutions are monitored, and new Security Technologies are researched. These ingredients converge on an annual basis into a strategic security plan that governs corporate information security strategy and product security related practices. These plans then influence initiatives, projects, policies and procedures across the company.

49. PSC's security policy is comprised of "a family of Information Security Policy documents that take the form of policies, standards, and procedural guidelines. Each of these types

[40] https://www.progress.com/security/information-security-program-whitepaper (last visited August 3, 2023).

of document are published inside of progress to shape employee behaviors, maintain the security of our environment, and the security of our products. Such documents are kept in an electronic policy binder and made available to all employees."[41]

50. Likewise, PSC's security policy is targeted at its products to prevent vulnerabilities from being exploited:[42]

## Product Security

All software products at progress are developed a via the use of modern methodologies, techniques, technologies, and processes. Our software development life cycles employ Agile methodologies while including numerous waves of security planning and testing. These include security requirements planning, security design planning, code level security scanning, vulnerability scanning, and penetration testing.

## Threat and Vulnerability Management

Ongoing threat and vulnerability management activities performed on all corporate assets and customer facing product environments. These activities include monitoring of key government and media outlets to stay apprised of emerging security issues, vulnerability scanning of internal and external systems, penetration testing of products and corporate environments.

51. As evidenced by, *inter alia*, their receipt of the notice from PSC informing them that their PII and PHI were compromised in the Data Breach, Plaintiff's and class members' PII and/or PHI was transferred using PSC's MOVEit service and thereby they entrusted Defendant with their PII and/or PHI, from which Defendant profited.

52. Yet, contrary to Defendant's website representations—by virtue of Defendant's admission that it experienced the Data Breach which revealed the PII and PHI of more than 37 million individuals—Defendant did not have adequate measures in place to protect and maintain sensitive PII and PHI entrusted to it.[43] Instead, Defendant's website wholly fails to disclose the truth: that Defendant lacks sufficient processes to protect the PII and PHI that is entrusted to it.

[41] *Id.*
[42] *Id.*
[43] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html

**B. The Data Breach**

53. On or around May 31, 2023, Defendant reported a vulnerability in its MOVEit Transfer and MOVEit Cloud systems that it said "could lead to escalated privileges and potential unauthorized access." On or about that same day, PSC purportedly notified all customers, and assigned a severity rating of 9.8 out of 10 to this vulnerability.

54. On or around June 9, 2023, PSC and its contracted cybersecurity firm, Huntress, uncovered additional vulnerabilities "distinct from the previously reported vulnerability" shared on May 31, 2023.

55. It has been reported by organizations using MOVEit software that were affected by the Breach that PII and PHI were stolen, including name, address, SSN, birthdate, height, eye color, driver's license number, vehicle registration information, handicap placard information, clinical information, demographic information, and financial health information (such as insurance billing information), among others.[44] Upon information and belief, the compromised information includes sensitive medical records and information related to health care and visits.

56. The Data Breach resulted from Defendant's failure to adequately protect and safeguard the highly sensitive PII and PHI entrusted to it.

57. As noted above, it is believed that the Data Breach was a ransomware attack conducted by C10p, which itself claims to have committed the Data Breach.[45]

58. Through its hack of PSC's MOVEit service, C10p claims to have stolen PII and PHI information from over 550 organizations and 37 million individuals, including U.S. schools,

[44] https://www.expresslane.org/alerts/ (last visited August 3, 2023).

[45] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (last visited August 3, 2023).

the U.S. public sector, and the U.S. private sector.[46] C10p is a well-known ransomware group, which "[has] been linked to FIN11, a financially-motivated cybercrime operation" and is "connected to both Russia and Ukraine and which is believed to be part of a larger umbrella operation known as TA505."[47]

59. It has been reported that C10p has requested unspecified ransom from organizations impacted by the MOVEit Data Breach in exchange for C10p to abstain from releasing consumers' highly sensitive PII and PHI. As of July 19, 2023, C10p and its hacking of MOVEit has resulted in the theft of more than 37 million individuals' sensitive information.[48] Because the Data Breach was conducted by known, self-proclaimed ransomware hackers, Plaintiff's and class members' sensitive PII and PHI are irrefutably in the possession of bad actors.

60. C10p posted a statement on its website demanding ransom from all companies impacted by the PSC MOVEit data breach, stating that if they refused to pay the ransom, C10p would post the sensitive PII and PHI stolen from Defendant's systems on the dark web[49]:

[46] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[47] *Id*.
[48] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[49] *See supra* n.46

***DEAR COMPANIES.***

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

***IMPORTANT!*** WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

***STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.***
***STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM***
***STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR***

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

***STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE***
***STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU***
***STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE***
***STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING***
***STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED***
***STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION***
***STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH***

***WHAT WARRANTY?*** OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

***FRIENDLY CLOP.***

***PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.***

61. Because the Data Breach was conducted by known, self-proclaimed ransomware cybercriminals, Plaintiff's and class members' sensitive PII and PHI are irrefutably in the possession of known bad actors. Furthermore, Plaintiff's and class members' PII and PHI are already listed for sale on the dark web, which places them at imminent risk that their data will be misused.

62. As explicitly acknowledged and stated on its own website, Defendant owed duties to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII and PHI against unauthorized access and disclosure, and to promptly notify individuals of any breach involving their information. Defendant breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect PII and PHI from unauthorized access and disclosure.

**C. Defendant Knew that Criminals Target PII and PHI**

63. At all relevant times, Defendant knew, or should have known, the PII and PHI of individuals whose information was transferred using MOVEit—such as Plaintiff and the class members—were a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and class members' information from cyber-attacks that Defendant should have anticipated and guarded against.

64. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were

758 medical data breaches in 2020 with over 40 million patient records exposed.[50] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[51]

65. PII and PHI are valuable property rights.[52] The value of this information as a commodity is measurable.[53] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[54] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[55] It is so valuable to identity thieves that once PII or PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

66. As a result of the real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII, PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[50] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Nov. 15, 2021).
[51] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Nov. 15, 2021).
[52] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data
[53] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[54] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.
[55] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

67. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[56] A cyber criminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[57] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[58]

68. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[59] According to a report released by the FBI's Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[60]

69. Criminals can use stolen PII and PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[61] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and

---

[56] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[57] *Id.*

[58] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[59] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[60] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[61] *What Happens to Stolen Healthcare Data*, *supra* at n.10.

extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[62]

70. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[63]

71. Given these facts, any company that transacts business with a consumer and then compromises the privacy of that consumer's PII or PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

**D. Theft of PII and PHI Has Grave and Lasting Consequences for Victims**

72. Theft of PII and PHI is serious. The FTC warns consumers that identity thieves use PII and PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[64]

73. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[65] According to Experian, "[t]he

---

[62] *Id.*

[63] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[64] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[65] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things,

research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[66]

74. With access to an individual's PII or PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[67]

75. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[68]

---

"[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[66] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[67] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).

[68] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).

76. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

77. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[69]

78. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[70] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[71] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII and PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[72] The FTC also warns, "If the thief's health information is mixed with yours,

[69] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[70] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf
[71] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.
[72] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 15, 2021).

your treatment, insurance and payment records, and credit report may be affected."[73]

79. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought or received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[74]

80. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[75]

81. It is within this harsh and dangerous reality that Plaintiff and all other class

[73] *Id*.
[74] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.
[75] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

members must now live with the knowledge that their PII and PHI are forever in cyberspace and were taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

**E. Damages Sustained by Plaintiff and the Class Members**

82. Plaintiff and the class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

## CLASS ALLEGATIONS

83. Plaintiff brings this action on behalf of herself and the following classes:

> Nationwide Class: All residents of the United States whose PHI and/or PII was compromised as a result of the Data Breach.
>
> Illinois Subclass: All residents of Illinois whose PHI and/or PII was compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class." Excluded from the Class are: (1) the judges presiding over the action, Class Counsel, and members of their families; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

84. **Numerosity**: Class members are so numerous that their individual joinder is

impracticable, as the proposed Class includes at least 37 million members who are geographically dispersed.

85. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Defendant's uniform misconduct, and Plaintiff's claims are identical to the claims of the class members she seeks to represent.

86. **Adequacy**: Plaintiff's interests are aligned with the Class she seeks to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and her counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

87. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other class members' claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendant's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

88. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and class members' PII and PHI from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and class members' PII and PHI;

c. Whether Defendant breached its duties to protect Plaintiff's and class members' PII and PHI;

d. Whether Defendant violated the statutes alleged herein;

e. Whether Plaintiff and the class members are entitled to damages and the measure of such damages and relief.

89. Given that Defendant engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE
### (On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)

90. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

91. Defendant owed duties to Plaintiff and the class members to exercise reasonable care in safeguarding and protecting their PII and PHI in Defendant's possession, custody, or control.

92. Defendant knew the risks of collecting and storing Plaintiff's and the class members' PII and PHI and the importance of maintaining secure systems. Defendant knew of the

many data breaches that targeted healthcare providers in recent years.

93. Given the nature of Defendant's business, the sensitivity and value of the PII and PHI it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

94. Defendant breached its duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII and PHI entrusted to it—including Plaintiff's and class members' PII and PHI.

95. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and class members' PII and PHI to unauthorized individuals.

96. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and class members, their PII and PHI would not have been compromised.

97. As a result of Defendant's above-described wrongful actions, inactions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and the class members have suffered, and will continue to suffer, economic damages and other injuries and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the

confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

**COUNT II**
**NEGLIGENCE PER SE**
**(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)**

98. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

99. Defendant's duties arise from, inter alia, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

100. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII and PHI.

101. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and the class members' PII and PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII and PHI including, specifically, the substantial damages that would result to Plaintiff and the other class members.

102. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

103. Plaintiff and class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

104. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

105. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and class members' PII and PHI to unauthorized individuals.

106. The injury and harm that Plaintiff and the other class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

**COUNT III**
**INVASION OF PRIVACY**
**(INTRUSION UPON SECLUSION)**
**(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)**

107. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

108. The State of Illinois recognizes the tort of Invasion of Privacy.

109. Plaintiff and class members had a reasonable expectation of privacy in the PII and PHI that Defendant failed to safeguard and allowed to be accessed by way of the Data Breach.

110. Defendant's conduct as alleged above intruded upon Plaintiff's and class members' seclusion under common law.

111. By intentionally and/or knowingly failing to keep Plaintiff's and class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and class members' private affairs in a manner that identifies Plaintiff and class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and class members.

112. Defendant knew that an ordinary person in Plaintiff's and the class members' position would consider Defendant's intentional actions highly offensive and objectionable.

113. Defendant invaded Plaintiff and class members' right to privacy and intruded into Plaintiff's and class members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

114. Defendant intentionally concealed from Plaintiff and class members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

115. As a proximate result of such intentional misuse and disclosures, Plaintiff's and class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

116. In failing to protect Plaintiff's and class members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private.

117. As a direct and proximate result of the foregoing conduct, Plaintiff seeks an award of damages on behalf of herself and the Class.

**COUNT IV**
**UNJUST ENRICHMENT**
**(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)**

118. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

119. Plaintiff and the class members have both a legal and equitable interest in their PHI and PII that was collected by, stored by, and maintained by Defendant—thus conferring a benefit upon Defendant—that was ultimately compromised by the Data Breach.

120. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and class members. Defendant also benefitted from the receipt of Plaintiff's and class members'

PHI and PII.

121. As a result of Defendant's failure to safeguard and protect PII and PHI, Plaintiff and class members suffered actual damages.

122. Defendant should not be permitted to retain the benefit belonging to Plaintiff and class members because Defendant failed to adequately implement the data privacy and security procedures that were mandated by federal, state, and local laws and industry standards.

123. Defendant should be compelled to provide for the benefit of Plaintiff and class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

**COUNT V**
**DECLARATORY RELIEF**
**(28 U.S.C. § 2201)**
**(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Illinois Subclass)**

124. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

125. An actual controversy has arisen and exists between Plaintiff and class members, on the one hand, and Defendant on the other hand, concerning the Data Breach and Defendant's failure to protect Plaintiff's and class members' PHI and PII, including with respect to the issue of whether Defendant took adequate measures to protect that information. Plaintiff and the Class are entitled to judicial determination as to whether Defendant has performed and is adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and class members' PHI and PII from unauthorized access, disclosure, and use.

126. A judicial determination of the rights and responsibilities of the parties regarding Defendant's privacy policies and whether it failed to adequately protect PHI and PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the Class, and so that there

is clarity between the parties as to Defendant's data security obligations with respect to PHI and PII going forward, in view of the ongoing relationships between the parties.

**COUNT VI**
**VIOLATIONS OF ILLINOIS PERSONAL INFORMATION PROTECTION ACT ("PIPA"), 815 ILCS 530/10(a)**
**(On behalf of Plaintiff and the Illinois Subclass)**

127. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

128. Section 10(b) of PIPA states, in pertinent part:

> [a]ny data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

815 ILCS 530/10(b).

129. Defendant is a "data collector" as defined by the statute; it is a software company that "handles, collects, disseminates, or otherwise deals with nonpublic personal information." 815 ILCS 530/5.

130. Plaintiff's and the Illinois Subclass members' claims are based on their statuses as "owner[s]" of their personal information.

131. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

132. Section 45 of PIPA requires entities who maintain or store "personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."

133. Defendant's conduct violated PIPA because Defendant voluntarily undertook the

act of maintaining and storing Plaintiff's PII and/or PHI, but failed to implement safety and security procedures and practices sufficient enough to protect from the Data Breach that it should have anticipated.

134. Defendant should have known and anticipated that data breaches were on the rise and that software companies were lucrative or likely targets of cyber criminals looking to steal PII and PHI. Therefore, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the Data Breach.

135. As a result of Defendant's violation of PIPA, Plaintiff and the Illinois Subclass incurred economic damages, including expenses associated with necessary credit monitoring.

## PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as Class Representative and undersigned counsel as Class Counsel;

B. Award Plaintiff and the Class actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity.

**JURY TRIAL DEMANDED**

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: August 3, 2023

Respectfully submitted,

By: */s/ Randi Kassan*

Randi Kassan
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

Gary M. Klinger (*Pro Hac Vice* forthcoming)
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

E. Michelle Drake (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
Email: emdrake@bm.net

Mark B. DeSanto (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdesanto@bm.net

*Attorneys for Plaintiff*